Securing Information in the Healthcare Industry: Network Security, Incident Management, and Insider Threat

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Greg Porter and Randy Trzeciak
September 23, 2010

http://www.cert.org/insider_threat/

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE
23 SEP 2010

2. REPORT TYPE

3. DATES COVERED
00-00-2010 to 00-00-2010

4. TITLE AND SUBTITLE
Securing Information in the Healthcare Industry: Network Security, Incident Management, and Insider Threat

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Carnegie Mellon University ,Software Engineering Institute,Pittsburgh,PA,15213

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

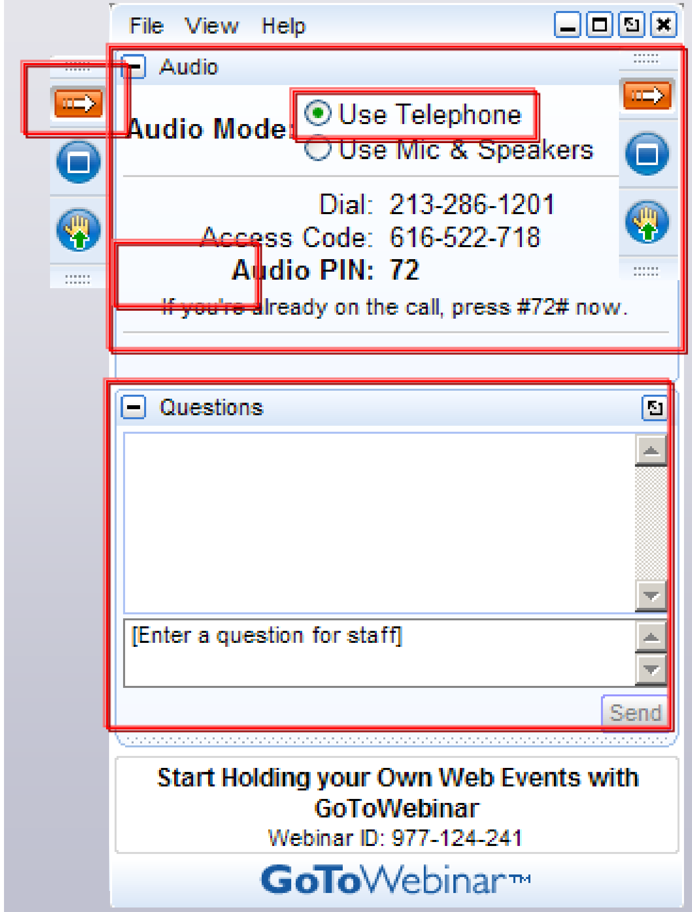
13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**25**	

How to Participate Today



Audio Mode: ● Use Telephone ○ Use Mic & Speakers

Dial: 213-286-1201
Access Code: 616-522-718
Audio PIN: 72
If you're already on the call, press #72# now.

[Enter a question for staff]

Start Holding your Own Web Events with GoToWebinar
Webinar ID: 977-124-241

- Open and close your Panel
- View, Select, and Test your audio
- Submit text questions
- Q&A addressed at the end of today's session

About the Speakers

Greg Porter is an Adjunct Professor at Heinz College at Carnegie Mellon University where he teaches information security and privacy related subject matter within the college's expanding graduate level health care programs. Greg is also the founder of Allegheny Digital, a Western Pennsylvania based security and privacy services company specializing in Network Infrastructure Security, Digital Forensics, Regulatory Compliance, and Enterprise Risk Management.

Prior to starting Allegheny Digital, Greg led the Mid Atlantic Information Protection & Business Resiliency Practice for KPMG, LLP, where he assumed various responsibilities ranging from Technical Lead to Project Manager. Greg maintains several information security related certifications and is a Certified Information Systems Security Professional (CISSP) and a Certified Information Security Manager (CISM). He also serves as a Visiting Scientist at SEI-CERT.

Randy Trzeciak is currently a senior member of the technical staff at CERT. He leads the insider threat team, which focuses on insider threat research; threat analysis and modeling; assessments; and training. Randy has more than 20 years of experience in software engineering; database design, development, and maintenance; project management; and information security. He also is an adjunct professor at Carnegie Mellon's Heinz College, School of Information Systems and Management.   Randy holds an MS in Management from the University of Maryland, a BS in Management Information Systems, and a BA in Business Administration from Geneva College.

Polling Question

#1 How did you hear about this webinar?

1. Social Media site (LinkedIn, Twitter)
2. Email invitation from the SEI
3. SEI Website
4. Website with webinar calendar i.e. www.webinar-directory.com
5. Other

Agenda

- Introduction
- Current State
- Threat Landscape
- Defensive Strategies
- Conclusion

Greg Porter

This Presentation

- Based on technical and non-technical health care security assessment observations
- Experience with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH)
- Trying to get a feel for health care security trends, as well as general infosec developments, observed during this time
- This presentation is directly affected by regulatory changes…new and old
- Intent is to simply provide an overview and perhaps provide some important considerations for organizations, health care based and otherwise

Agenda

- Introduction
- Current State
- Threat Landscape
- Defensive Strategies
- Conclusion

Current State

- Where are we today?
- 14 years after the passage of HIPAA
- Over 5 years since Covered Entities had to be compliant with the HIPAA Security Rule
- The HITECH Act and Business Associate compliance demands
- A year since the breach notification requirements (IFR)
- Meaningful use & electronic health records (EHR)
- Yet…we continue to see health care organizations struggle with the governance and security of electronic protected health information (ePHI)

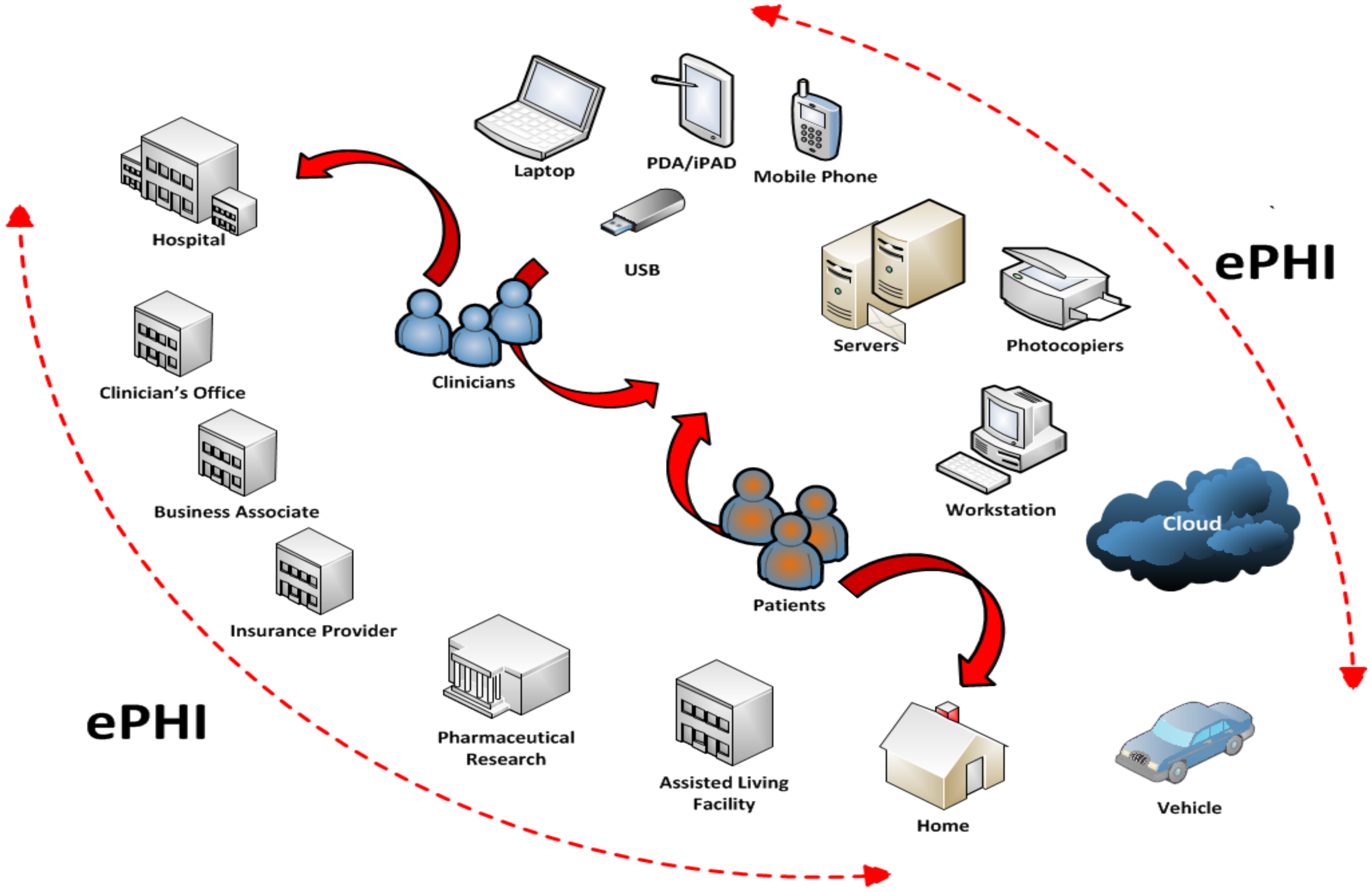
Regulatory Demands

- **Regulations driving industry compliance**
  - HIPAA Security
  - HIPAA Privacy
  - HITECH Act
  - Payment Card Industry Data Security Standards (PCI-DSS)
  - Genetic Information Non-discrimination Act (GINA)
  - FTC Red Flags Rule?
  - State Regulations & Breach Notification Requirements
- **Regulatory compliance merely sets the floor, be mindful of the "set it and forget it" mindset**

Beyond ePHI

- HIPAA Security, that’s new right?
- Breach notification concerns awakening *Accountability Act* components of HIPAA Security
- Prior to 2008, HIPAA Security enforcement was scant, but that’s dramatically changing
- Data is the new currency
  - HIPAA Privacy – PHI
  - HIPAA Security – ePHI
  - Unsecured PHI – HITECH Act
  - Cardholder Data – PCI DSS
  - Personal Data – State Regulations
- The protection of ePHI is a challenge in even the most well managed environments, but why?

The Unbounded Health Care Enterprise

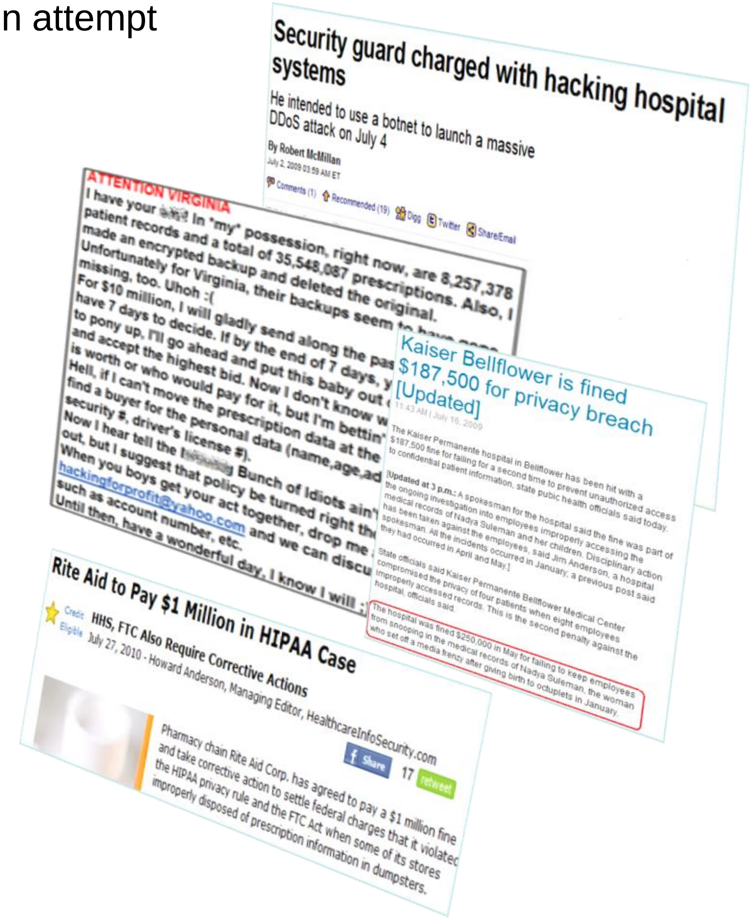


Agenda

- Introduction
- Current State
- Threat Landscape
- Defensive Strategies
- Conclusion

Threat Landscape

- **External attacks**
  - Virginia Health Professions Database
  - 8 million patient records compromised, $10 million extortion attempt
- **Insider Threats**
  - Security guard charged with hacking hospital systems
  - Planned massive July 4, DDoS attack
  - Janitor, Northwestern Memorial Hospital
- **Physical Security**
  - CVS & Rite Aid disposal practices
  - Throwing away confidential medical information into unsecured dumpsters
  - HIPAA violation, fined $2.25 million
- **Regulatory Enforcement**
  - Insurer Health Net will pay $250,000 in damages and offer stronger consumer protections
  - Connecticut Attorney General Richard Blumenthal



Security guard charged with hacking hospital systems

He intended to use a botnet to launch a massive DDoS attack on July 4

By Robert McMillan
July 2, 2009 03:59 AM ET

ATTENTION VIRGINIA
I have your [redacted]! In "my" possession, right now, are 8,257,378
patient records and a total of 35,548,087 prescriptions. Also, I
made an encrypted backup and deleted the original.
Unfortunately for Virginia, their backups seem
missing, too. Uhoh :(
For $10 million, I will gladly send along the pas
have 7 days to decide. If by the end of 7 days, y
to pony up, I'll go ahead and put this baby out
and accept the highest bid. Now I don't know w
is worth or who would pay for it, but I'm bettin'
Hell, if I can't move the prescription data at the
find a buyer for the personal data (name,age,ad
security #, driver's license #).
Now I hear tell the [redacted] Bunch of Idiots ain't
out, but I suggest that policy be turned right th
When you boys get your act together, drop me
hackingforprofit@yahoo.com and we can discu
such as account number, etc.
Until then, have a wonderful day, I know I will ;)

Kaiser Bellflower is fined $187,500 for privacy breach [Updated]

11:43 AM | July 16, 2009

The Kaiser Permanente hospital in Bellflower has been hit with a $187,500 fine for failing for a second time to prevent unauthorized access to confidential patient information, state pubic health officials said today.

[**Updated at 3 p.m.:** A spokesman for the hospital said the fine was part of the ongoing investigation into employees improperly accessing the medical records of Nadya Suleman and her children. Disciplinary action has been taken against the employees, said Jim Anderson, a hospital spokesman. All the incidents occurred in January; a previous post said they had occurred in April and May.]

State officials said Kaiser Permanente Bellflower Medical Center compromised the privacy of four patients when eight employees improperly accessed records. This is the second penalty against the hospital, officials said.

The hospital was fined $250,000 in May for failing to keep employees from snooping in the medical records of Nadya Suleman, the woman who set off a media frenzy after giving birth to octuplets in January.

Rite Aid to Pay $1 Million in HIPAA Case

Credit Eligible **HHS, FTC Also Require Corrective Actions**
July 27, 2010 - Howard Anderson, Managing Editor, HealthcareInfoSecurity.com

Pharmacy chain Rite Aid Corp. has agreed to pay a $1 million fine and take corrective action to settle federal charges that it violated the HIPAA privacy rule and the FTC Act when some of its stores improperly disposed of prescription information in dumpsters.

Breach

- **Data anywhere ≠ data everywhere**
- Over 110 breaches affecting more than 4.1M individuals and health records have occurred since the HIPAA Breach Notification Rule took effect on September 23, 2009[1]
  - Ponemon Institute[2] - average cost per compromised record is $144—$204 of indirect costs and $60 of direct costs
  - To date, the theft of laptops is the primary cause of a breach of ePHI, followed by the theft of desktop computers and theft of removable media
  - Hacking incidents have also led to breaches
- U.S. Department of Health and Human Services, Breaches Affecting 500 or More Individuals
  - http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html

[1] Hourihan, Chris, "*An Analysis of Breaches Affecting 500 or More Individuals in Healthcare*", HITRUST, August 2010.

[2] "2009 Annual Study: Cost of a Data Breach," Ponemon Institute LLC, January 2010.

Motivation

- **Organized crime**
  - While a hacker might get 40 cents for a stolen credit card number, a stolen medical identity could fetch a premium of $14 to $18
- **Medical identity theft**
  - Patient pretends to be someone else so they won't have to pay for their own medical bills
  - Organized thieves working as receptionists, janitors, and accountants within the health care field itself
- **Health care entities have valuable assets**
  - Like electronic medical records on most of us
  - Information rich environments, not just ePHI and PII, also financial data, R&D information, academic studies,
  - Equipment (e.g. laptops, PDA’s, mobile phones, robots)

Health Care Targeting

- Hacker Attacks Targeting Health Care Organizations Doubled in the 4th Quarter of 2009
  - SecureWorks Data
- Attempted attacks increased from an average of 6,500 per health care client per day in the first nine months of 2009 to an average of 13,400 per client per day in the last three months of 2009
- Attempted attacks against other types of organizations, protected by SecureWorks, did not increase in the fourth quarter
- Possible correlation?

Impact

- Breach of ePHI
- Damage to reputation
- Regulatory consequence and financial penalties
- Jail time, criminal penalties for willful neglect
- ***Loss of human life?***
  - While many concerns focus on a data breach, some vulnerabilities can be more severe
  - Pacemakers and implantable cardiac defibrillators susceptible to RF manipulation and attack[1]
  - Consider the implications of previously mentioned DDoS attack and availability of WiFi equipped IV infusion pumps

[1] Feder, Barnaby, "*A Heart Device Is Found Vulnerable to Hacker Attacks*", New York Times, March, 2008, http://www.futurecrimes.com/biological-human-genome-crime/hacking-the-human-heart-medical-devices-found-subject-to-technical-attack/

Polling Questions

# 2 Has your organization conducted a HIPAA security assessment within the past 18 months? YES / NO

# 3 Does management have a definitive understanding of where, exactly, electronic protected health information is located within the organization? YES / NO

Social Networks

- Consider the benefits…and the risks!
  - Social networks foster collaboration and cohesion
  - Also one of the leading sources of malware infection
- More and more, provider and payer reputations are available on line, including patient / customer opinions and ratings
- Henry Ford Hospital “tweets” live procedure during kidney surgery[1]
- Raise awareness, assist patients, text4baby program
- http://www.text4baby.org
- Communicate during crisis events
  - November, 2009 Fort Hood shooting attack
  - Scott & White Healthcare – one of the hospitals that treated Fort Hood victims, used Twitter to provide up-to-the-minute news
  - Organize personnel during natural disasters, TN and IA

[1] http://www.cnn.com/2009/TECH/02/17/twitter.surgery/index.html

Social Network Risks

- Major source for malware infections
- Consider user behaviors
  - Tri-City Medical Center in Oceanside, CA
  - Summer, 2010
  - 5 employees fired for posting patient information online Facebook
- Chicago, IL
  - Native American, Christopher Cornstalk
  - Battled alcoholism
  - RN started a page, "Did you Know this Alcoholic Indian?“
  - Shared unflattering photos of the patient, posted comments
  - Over 600 people joined, including RN’s, EMT's, Firefighters, and Police Officers
- Establish a social media policy, then monitor and enforce it
  - Set penalties for violating policy. For example, an intentional act of misusing or breaching patient information results in immediate dismissal

Cloud Computing

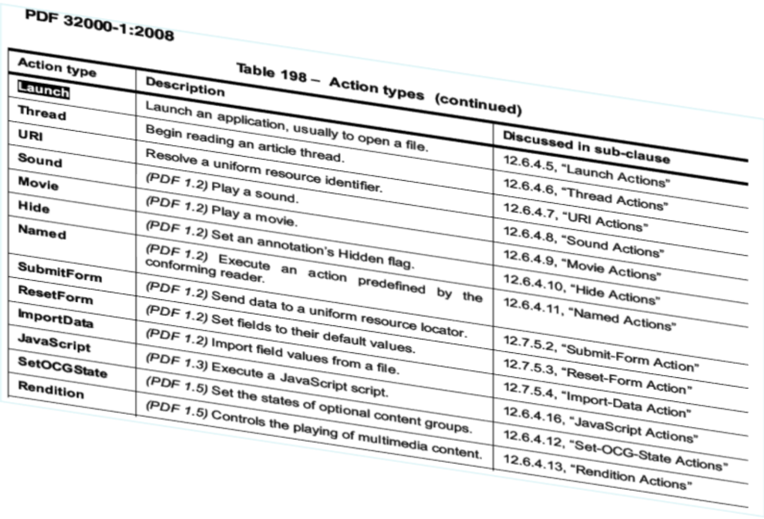
- “Cloud” offers rapid scalability and provisioning, but what it’s missing is quite important:
  - Cloud computing lacks standards about data handling and security practices
  - No agreement about whether a vendor has an obligation to tell users if their data is in the U.S. or not
  - Users and vendors are only beginning to try to sort out those issues through industry associations, such as the year-old Cloud Security Alliance
- Prior to reaching any agreement with a cloud provider, carefully review service level agreements and conduct thorough security reviews prior to finalizing

Emerging Threats

- **Today’s malware**
  - Very sophisticated, targeted, and designed to infect, conceal access, pilfer data and modify information without detection
- Client-side attacks, attacker targets an employee’s PC
  - Why? Compromise client device to gain network foothold and purview of whatever may be connected…such as data and other systems!
  - Workforce members PC may directly communicate with back-end systems containing sensitive data such as ePHI, PII, and CCD
  - Visibility - Provides attacker with a foothold to exploit other internal systems
- Exploited via application vulnerabilities
- Vulnerabilities that exist in widely deployed and commonly used programs such as IE, FireFox, Safari, Adobe Acrobat, MS Word, Excel, etc.

Malware – Client Side Exploitation

- Adobe PDF (Portable Document Format)
- Sometimes referred to as Problematic Document Format
- Highly useful, highly exploitable software
- Offers a well leveraged vehicle for client side attacks and inevitably compromising health care targets
- Why? Well attacker can all embed music, movies, 3D artwork complete with JavaScript, submit-form action (submit the data you input directly to a server somewhere on the Internet)
- Executable Files



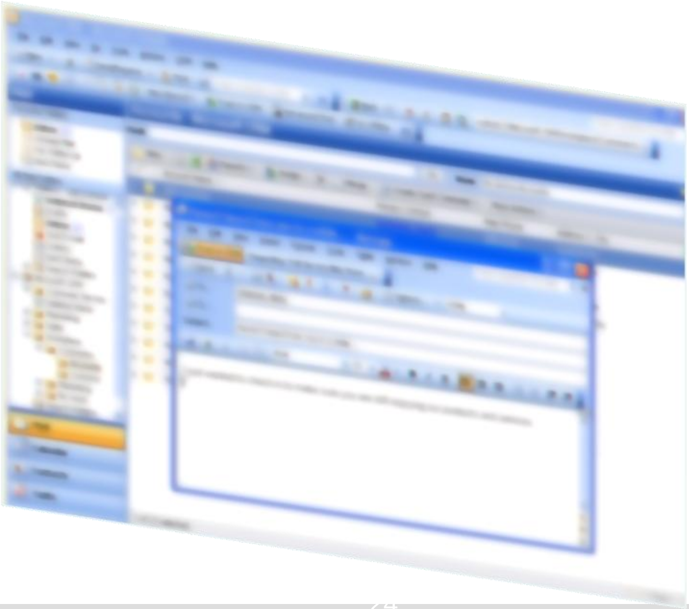
PDF 32000-1:2008

Table 198 – Action types (continued)

Action type	Description	Discussed in sub-clause
Launch	Launch an application, usually to open a file.	12.6.4.5, "Launch Actions"
Thread	Begin reading an article thread.	12.6.4.6, "Thread Actions"
URI	Resolve a uniform resource identifier.	12.6.4.7, "URI Actions"
Sound	*(PDF 1.2)* Play a sound.	12.6.4.8, "Sound Actions"
Movie	*(PDF 1.2)* Play a movie.	12.6.4.9, "Movie Actions"
Hide	*(PDF 1.2)* Set an annotation's Hidden flag.	12.6.4.10, "Hide Actions"
Named	*(PDF 1.2)* Execute an action predefined by the conforming reader.	12.6.4.11, "Named Actions"
SubmitForm	*(PDF 1.2)* Send data to a uniform resource locator.	12.7.5.2, "Submit-Form Action"
ResetForm	*(PDF 1.2)* Set fields to their default values.	12.7.5.3, "Reset-Form Action"
ImportData	*(PDF 1.2)* Import field values from a file.	12.7.5.4, "Import-Data Action"
JavaScript	*(PDF 1.3)* Execute a JavaScript script.	12.6.4.16, "JavaScript Actions"
SetOCGState	*(PDF 1.5)* Set the states of optional content groups.	12.6.4.12, "Set-OCG-State Actions"
Rendition	*(PDF 1.5)* Controls the playing of multimedia content.	12.6.4.13, "Rendition Actions"

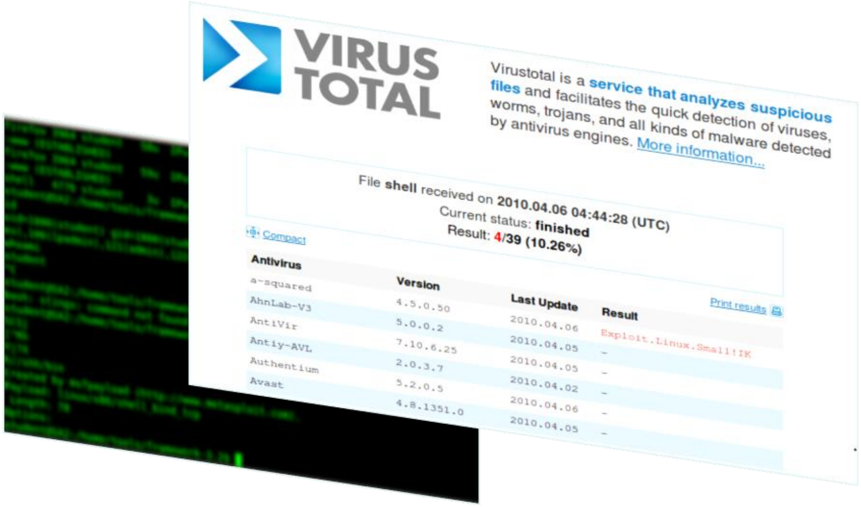
Malware Delivery

- How about e-mail?
- But our anti-virus software will catch that right?
  - Maybe not…good if you have a known signature in your AV database
  - Attackers often utilize publicly available, high quality tools such as the Metasploit framework to pack malicious code, scrambling the executable file in an effort to evade detection
- Can utilize Metasploit to create a reverse HTTP executable shell file
- May run over SSL to aid evasion



Malware – Detection

- Can use a service such as VirusTotal prior to sending a malicious file
- Will attempt to identify viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and web analysis toolbars across 40 different AV vendors
- Chances are, the target is running one of them
- So, if the payload is not detected by any of the vendors, may have increased the likelihood that a given user will execute the file



VIRUS TOTAL

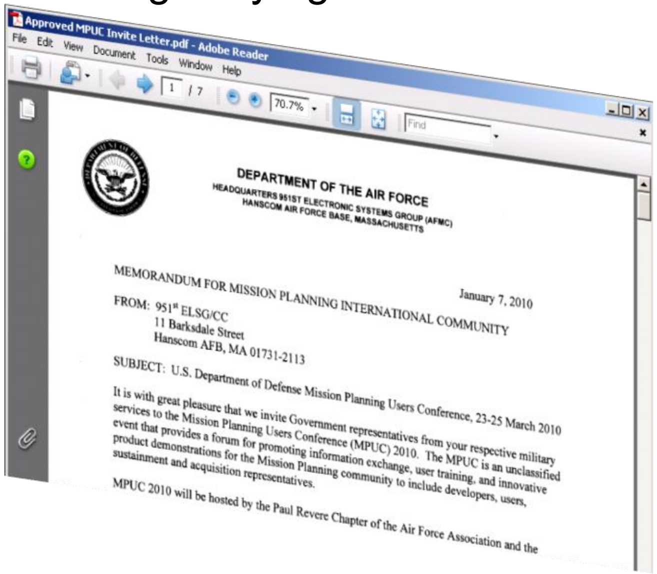
Virustotal is a service that analyzes suspicious files and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...

File shell received on 2010.04.06 04:44:28 (UTC)
Current status: finished
Result: 4/39 (10.26%)

Antivirus	Version	Last Update	Result
a-squared	4.5.0.50	2010.04.06	Exploit.Linux.Small!IK
AhnLab-V3	5.0.0.2	2010.04.05	-
AntiVir	7.10.6.25	2010.04.05	-
Antiy-AVL	2.0.3.7	2010.04.02	-
Authentium	5.2.0.5	2010.04.06	-
Avast	4.8.1351.0	2010.04.05	-

Malware – Client Side Delivery

- Malicious PDF files e-mailed to US defense contractors
  - The document talks about a real conference held in Las Vegas in March, 2010[1]
  - When opened to Adobe Reader, the file exploited the CVE-2009-4324 vulnerability
  - A backdoor connected to IP address 140.136.148.42. In order to avoid detection, it bypasses the local web proxy when doing this connection
  - Anybody who controls that IP will gain access to the infected computer and the company network. This particular IP is located in Taiwan
- It's reasonable to believe that similar attacks are occurring daily against health care entities


Approved MPUC Invite Letter.pdf - Adobe Reader
File Edit View Document Tools Window Help
1 / 7
70.7%
Find

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS 951ST ELECTRONIC SYSTEMS GROUP (AFMC)
HANSCOM AIR FORCE BASE, MASSACHUSETTS

January 7, 2010

MEMORANDUM FOR MISSION PLANNING INTERNATIONAL COMMUNITY

FROM: 951st ELSG/CC
11 Barksdale Street
Hanscom AFB, MA 01731-2113

SUBJECT: U.S. Department of Defense Mission Planning Users Conference, 23-25 March 2010

It is with great pleasure that we invite Government representatives from your respective military services to the Mission Planning Users Conference (MPUC) 2010. The MPUC is an unclassified event that provides a forum for promoting information exchange, user training, and innovative product demonstrations for the Mission Planning community to include developers, users, sustainment and acquisition representatives.

MPUC 2010 will be hosted by the Paul Revere Chapter of the Air Force Association and the

[1] http://www.f-secure.com/weblog/archives/00001859.html

More Vulnerabilities

- **Non-secure web applications**
  - Resulting in web based exploitation via cross site scripting (XSS), SQL injection, etc.
- **Misconfigured systems**
  - Internet facing (external) infrastructure, web/DMZ servers, switches, routers, terminal services, modems (yes, modems), etc
  - Internal systems, workstations, mobile devices
  - Wireless infrastructure (AP’s, Bluetooth]
  - Default passwords!
- **Sensitive information is everywhere & its location often not well understood**
  - Exists in structured areas such as databases, but also unstructured areas such as text files, Word/Excel, etc.
  - Unbounded networks & mobility
  - Vendors and business associates, how is data flow determined…definitively?
- **Poor patch management**
  - Both at the OS and application level

The Challenge

- Corporate information systems and data are under assault like never before
- Asymmetric issue, many :one
  - Health care entities must identify and then defend against (many) potential attack vectors within their environment, and then vigilantly monitor
  - Attackers only need to find a single weakness to exploit
- Automated attack tools and packaged exploits make this challenge all the more difficult to defend against
- Botnets, autonomous exploit kits, significantly reduces technical expertise needed…so easy a caveman could do it?
- Metasploit and other well developed, proven tools are free

Agenda

- Introduction
- Current State
- Threat Landscape
- Defensive Strategies
- Conclusion

HIPAA Security Drivers

- Use compliance drivers to your advantage
- As *required* by HIPAA’s Administrative Safeguard Standard
  - §164.308(a)(8), Evaluation
  - Perform a periodic technical and nontechnical evaluation that establishes the extent to which a given CE’s policies and procedures meet the intent of the HIPAA Security provisions
- Work with General Counsel to ensure that your current HIPAA Security posture is compliant with legislative intent
- Conduct an accurate and thorough risk assessment to identify, define, and prioritize risks to ePHI, should also encompass ePHI brokered to business associates

Defensive Considerations

- Integrate and/or align Breach Procedures with your Incident Response Plan, *you do have one right*? Then test it
- Consider formalized training on incident handling, including:
  - How to develop and manage a CSIRT
  - How to customize your CSIRT to meet the unique demands of the health care industry
- Restrict & monitor privileged users
- Baseline network traffic, what’s normal?
  - Filter and monitor outgoing traffic
  - Lock down outbound ports and services based on business justification
  - Do all users need access to Telnet, FTP, TFTP, SSH, RDP, etc.,
- If reasonable and appropriate, conduct penetration testing and vulnerability assessments (internal and external) against information assets storing or processing ePHI

Defensive Considerations

- Conduct an accurate and thorough risk assessment to identify, define, and prioritize risks to ePHI
- How do I perform a risk assessment?
  - NIST 800-30
  - SEI-CERT, OCTAVE
- Develop a thorough Monitoring process, including log collection and analysis
- Utilize biometrics to harden authentication processes, inhibiting the ability of password information being compromised
- Patch your systems & don’t run as ADMINISTRATOR (or Root) on your local workstation
- Realize you likely have users doing this every day…do you know who they are?
- Review service level agreements and contracts, ensure a “Right to Audit” clause is included
- Audit!

Governance Models

- Consider a business process oriented approach to information security
  - Frameworks such as the CERT Resilience Management Model (CERT-RMM)
  - Understand resilience across the organizations people, information, technology, and facilities
  - www.cert.org/resilience
- Check out the Health Information Trust Alliance (HITRUST)
  - Excellent source for health care related security controls
  - Based off of the ISO 27000 family of standards
  - www.hitrustalliance.net
- Education
  - Emphasize the lack of anonymity in your environment
  - Your activities can and may be monitored
  - Use real-world attacks and scams as examples
  - Encourage paranoia
  - Consider how your data is managed from entrance to exit

Polling Questions

# 4 Does your organization have an incident response plan? YES / NO

# 5 Does your incident response process account for the HITECH Acts Breach Notification requirements? YES / NO

Agenda

- Introduction
- Current State
- Threat Landscape
- Defensive Strategies
- Conclusion

Conclusion

- Health care organizations process and exchange highly sensitive patient information daily, leading to the potential for increased risk and exposure
- IP, PII, and ePHI is highly valued by the cyber criminal underground and will continue to be targeted
- It is the responsibility of assigned organizational management to take reasonable and appropriate measures to safeguard sensitive information in line with regulatory demands and consumer expectations
- Potential threats and risks to information should be accounted for prior to information security controls are developed, assessed, implemented, and monitored
- Strongly consider the people, information, technology and facilities that sustain critical operations and protect them commensurate to operational value and regulatory expectations, such as HIPAA/HITECH

Insider Threat Agenda

Introduction

How bad is the insider threat?

Exploration of each type of insider crime:

- IT sabotage
- Theft of Intellectual Property
- Fraud

Best Practice for Prevention and Detection

Discussion

Randy Trzeciak

Introduction

Who is a Malicious Insider?

Current or former employee, contractor, or other business partner who

- *has or had authorized access to an organization’s network, system or data and*
- *intentionally exceeded or misused that access in a manner that*
- *negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems.*

Types of Insider Crimes

Insider IT sabotage

An insider's use of IT to direct specific harm at an organization or an individual.

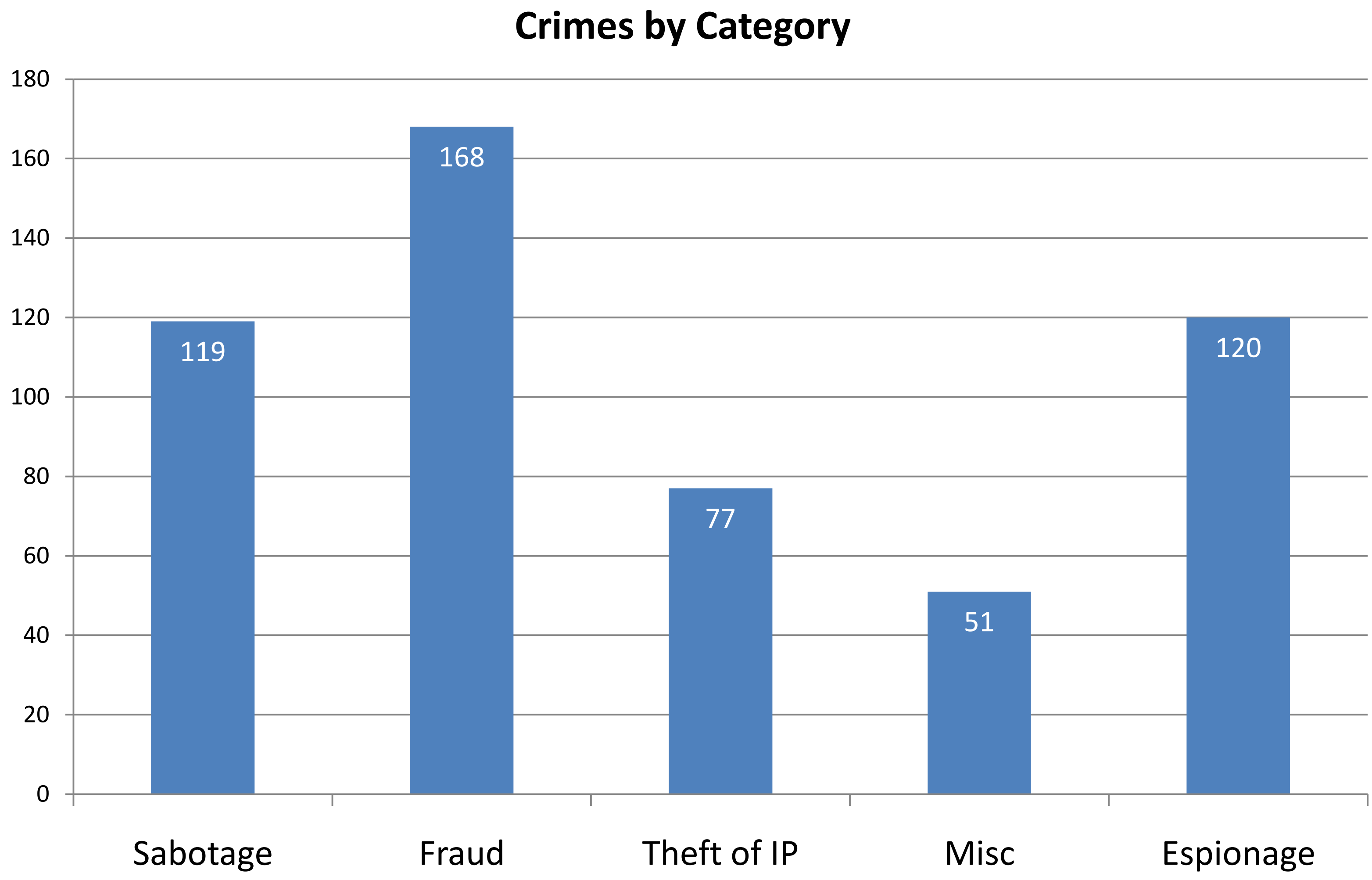
Insider theft of intellectual property (IP)

An insider's use of IT to steal intellectual property from the organization. This category includes industrial espionage involving insiders.

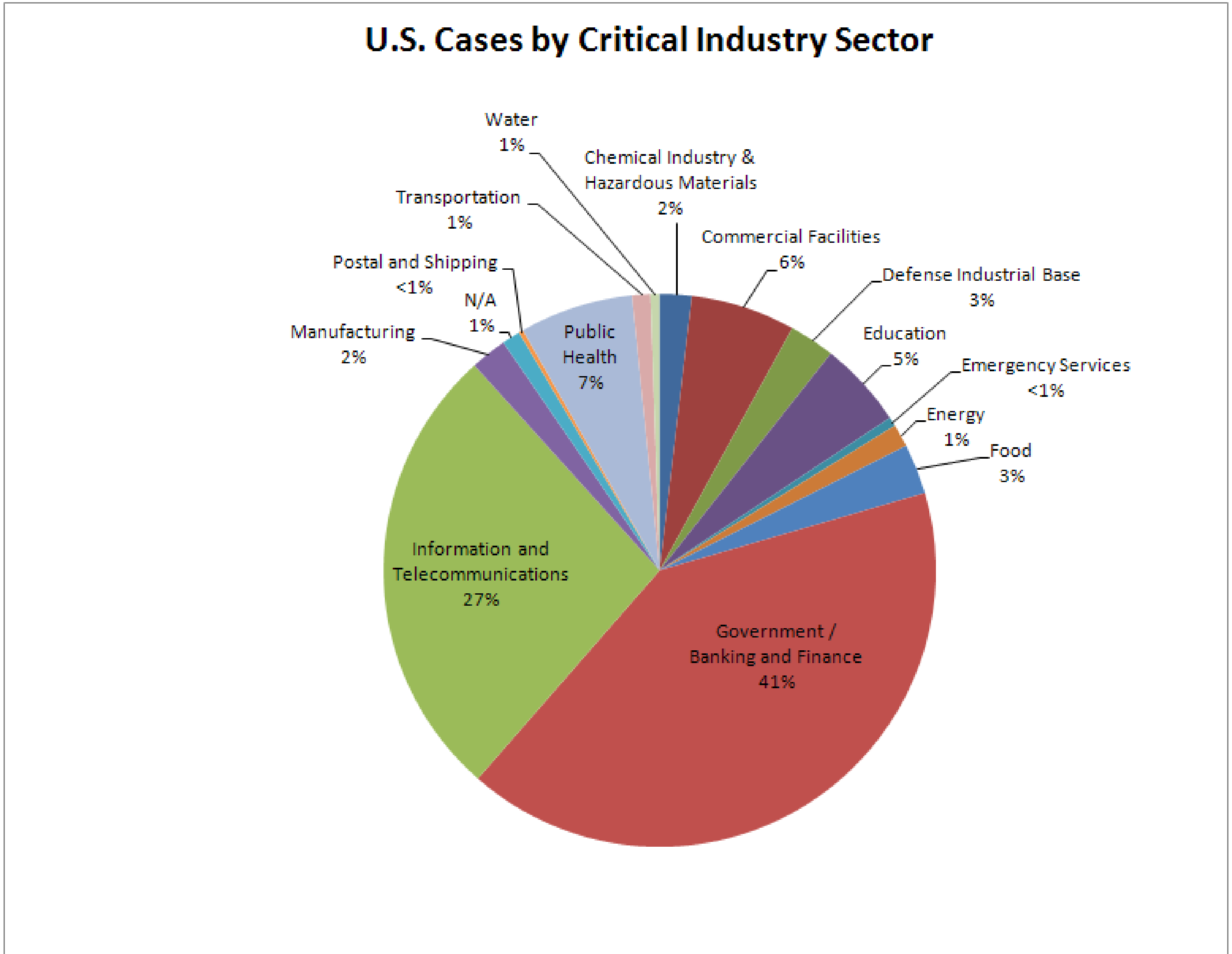
Insider fraud

An insider's use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or theft of information which leads to fraud (identity theft, credit card fraud).

CERT's Insider Threat Case Database



Critical Infrastructure Sectors



*** This does not include espionage cases involving classified information*

How bad is the insider threat?

Insider Threat Issue -1

Insiders pose a substantial threat by virtue of their knowledge of, and access to, their employers' systems and/or databases.

Insiders can bypass existing physical and electronic security measures through ***legitimate*** measures.

Polling Questions

# 6 Has your organization been the victim of an insider attack? YES / NO

# 7 Can you ***confidently*** say you have ***not*** been the victim of an insider attack?
YES / NO

2009 e-Crime Watch Survey

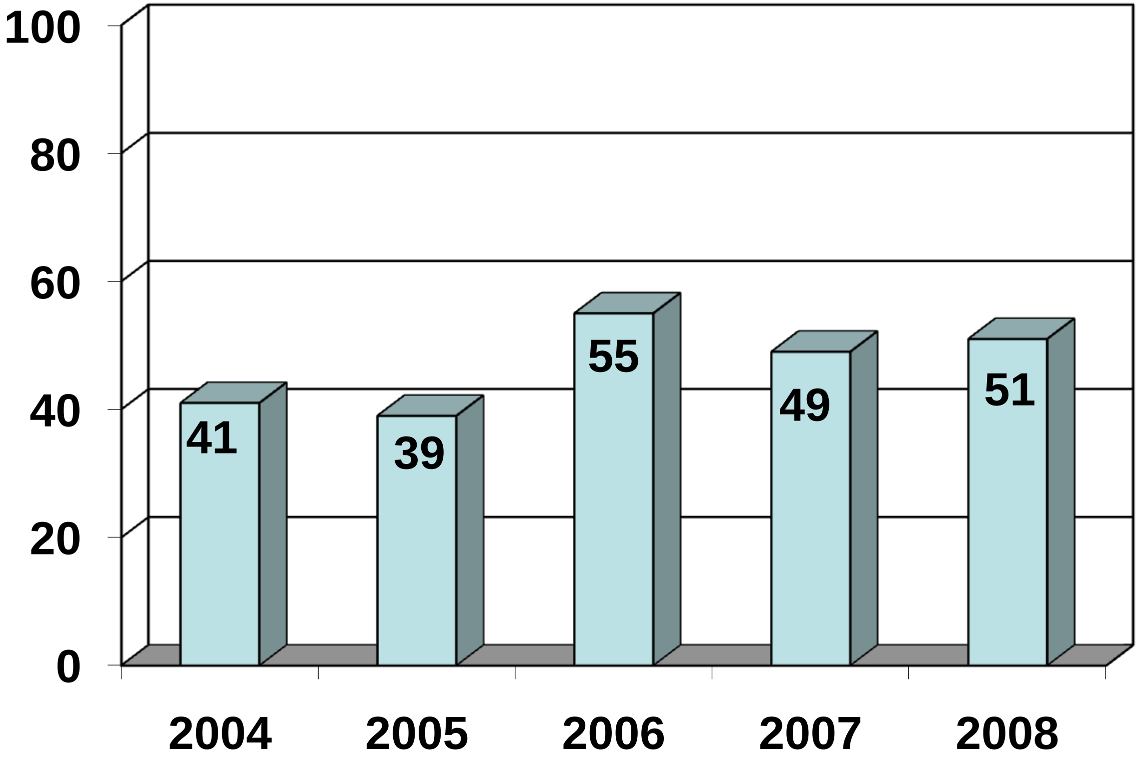
CSO Magazine, USSS, CERT & Deloitte

523 respondents

39% of organizations have less than 500 employees

23% of organizations have less than 100 employees

Percentage of Participants Who Experienced an Insider Incident



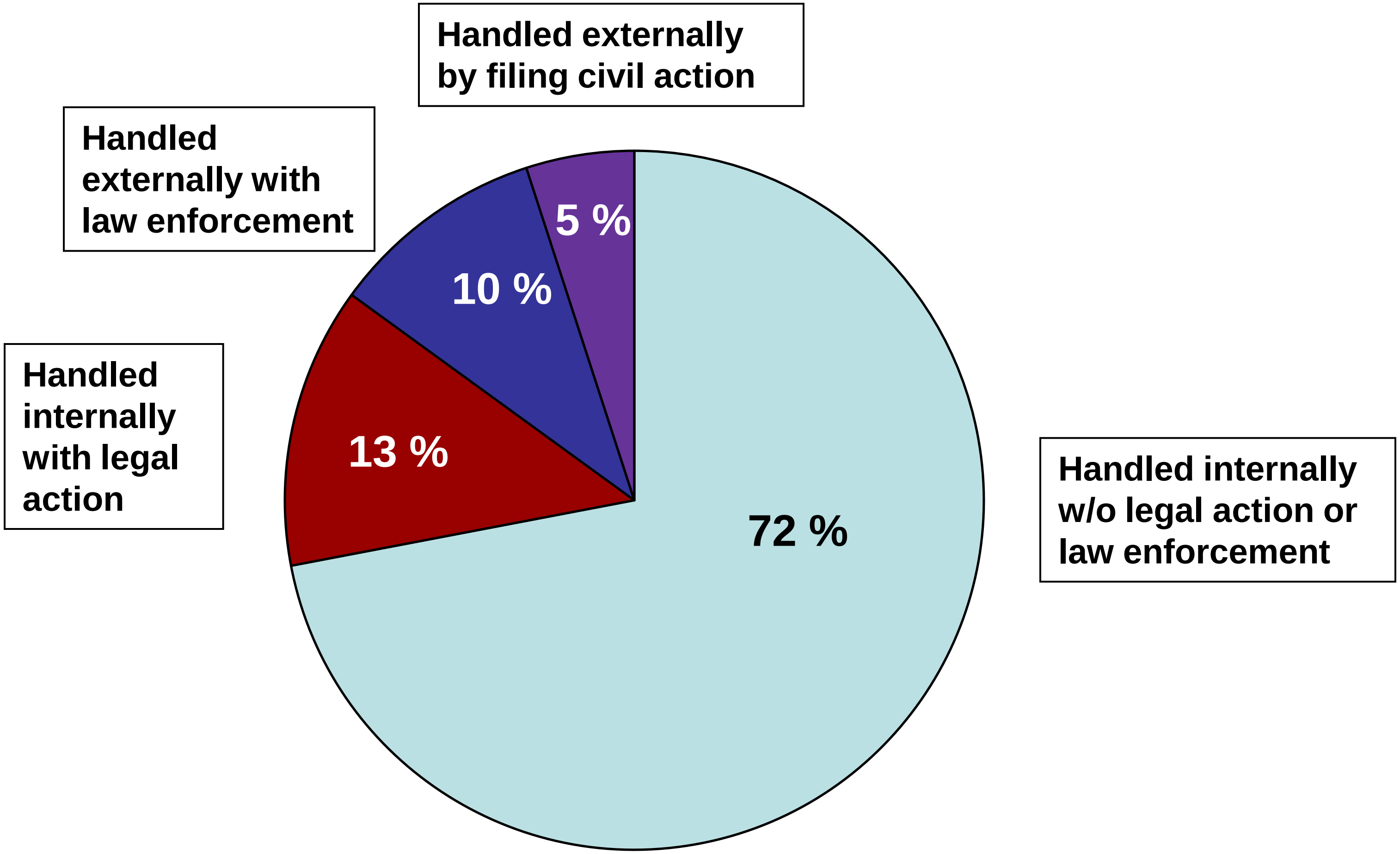
2009 e-Crime Watch Survey -2

43 % of respondents	Insiders posed the greatest cyber security threat to their organization during the past 12 months
67 % of respondents	Damage caused by insider attacks more damaging than outsider attacks
Most common insider e-crime	

Unauthorized access to / use of corporate information	(23%)
Theft of intellectual property	(16%)
Theft of other information (financial & customer data)	(15%)
Fraud	(11%)
Intentional exposure of private or sensitive data	(11%)

2009 E-Crime Survey Results - 3

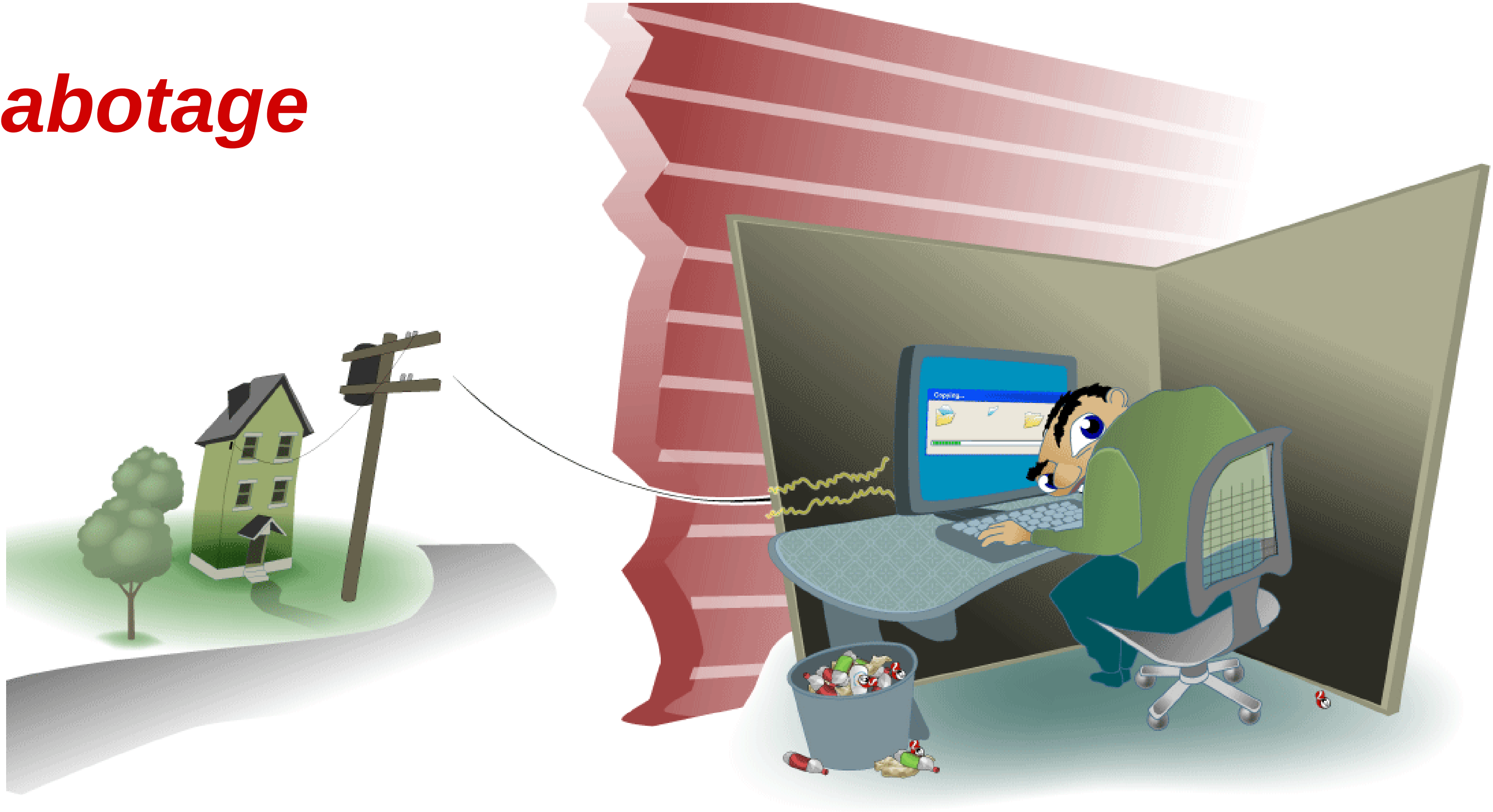
Which percentage of Electronic Crimes committed by insiders were:



Insider Crime Profiles

Crime Profile # 1

IT Sabotage



IT Sabotage Incidents

An IT consultant for a hospital medical supply facility seeks revenge when he loses control of his company

…System administrator sabotages systems on his way out

A security guard at a U.S. hospital, after submitting resignation notice, obtained physical access to computer rooms

…Installed malicious code on hospital computers, accessed patient medical records

Insider IT Sabotage

Who did it?

- Former employees
- Male
- Highly technical positions
- Age: 17 – 60

How did they attack?

- No authorized access
- Backdoor accounts, shared accounts, other employees' accounts, insider's own account
- Many technically sophisticated
- Remote access outside normal working hours

Summary of Findings

	IT Sabotage
% of crimes in case database	35%
Current or former employee?	Former
Type of position	Technical (e.g. sys admins or DBAs)
Gender	Male

Summary of Findings

	IT Sabotage
Target	Network, systems, or data
Access used	Unauthorized
When	Outside normal working hours
Where	Remote access
Recruited by outsiders	None
Collusion	None

Crime Profile # 2

Theft of Intellectual Property

WELCOME ABOARD SMITH. I'M SURE THE "KNOWLEDGE AND EXPERIENCE" YOU BRING WITH YOU WILL BE EXTREMELY VALUABLE.
CONFIDENTIAL
RESEARCH
PATENTS

Theft of Information Incidents

A technical operations associate at a pharmaceutical company downloads 65 GB of information, including 1300 confidential and proprietary documents, intending to start a competing company, in a foreign country…

Organization spent over $500M in development costs

Theft of Intellectual Property

Who did it?

- Current employees
- Technical or sales positions
- All male
- Average age: 37

What was stolen?

- Intellectual Property (IP)
- Customer Information (CI)

How did they steal it?

- During normal working hours
- Using authorized access

Dynamics of the Crime

Most were *quick* theft upon resignation

Stole information to

- Take to a new job
- Start a new business
- Give to a foreign company or government organization

Collusion

- Collusion with at least one *insider* in almost 1/2 of cases
- Outsider *recruited* insider in less than 1/4 of cases
- Acted *alone* in 1/2 of cases

Summary of Findings

	IT Sabotage	Theft of Intellectual Property
% of crimes in case database	35%	18%
Current or former employee?	Former	Current
Type of position	Technical (e.g. sys admins or DBAs)	Technical (71%) - scientists, programmers, engineers Sales (29%)
Gender	Male	Male

Summary of Findings

	IT Sabotage	Theft of Intellectual Property
Target	Network, systems, or data	IP (trade secrets) – 71% Customer Info – 33%
Access used	Unauthorized	Authorized
When	Outside normal working hours	During normal working hours
Where	Remote access	At work
Recruited by outsiders	None	Less than 1/4
Collusion	None	Almost ½ colluded with at least one insider; ½ acted alone

Crime Profile # 3

Fraud

Fraud Incidents

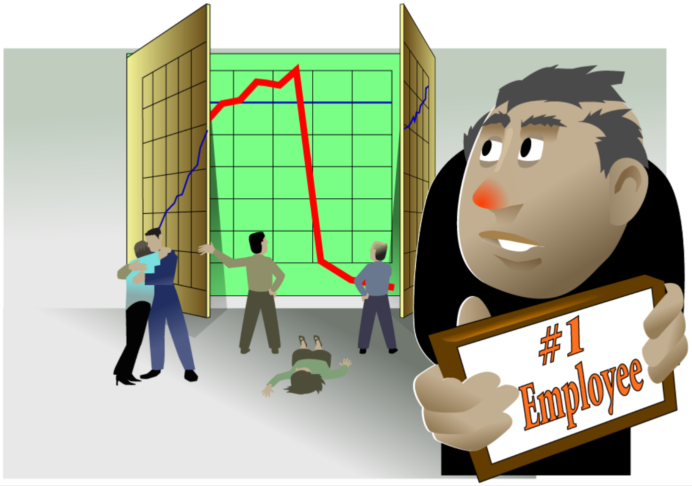
An accounts payable clerk, over a period of 3 years, issues 127 unauthorized checks to herself an others...

Checks totaled over $875,000

A front desk office coordinator stole PII from hospital...

Over 1100 victims and over $2.8 M

in fraudulent claims



Fraud: Theft or Modification

Most attacks were long, ongoing schemes

Who did it?

- Current employees
- “Low level” positions
- Gender: fairly equal split
- Average age: 33

What was stolen/modified?

- Personally Identifiable Information (PII)
- Customer Information (CI)
- Very few cases involved trade secrets

How did they steal/modify it?

- During normal working hours
- Using authorized access

Summary of Findings

	IT Sabotage	Theft of Intellectual Property	Fraud
% of crimes in case database**	35%	18%	40%
Current or former employee?	Former	Current	Current
Type of position	Technical (e.g. sys admins or DBAs)	Technical (71%) - scientists, programmers, engineers Sales (29%)	Non-technical, low-level positions with access to confidential or sensitive information (e.g. data entry, customer service)
Gender	Male	Male	Fairly equally split between male and female

***** Does not include national security espionage***

Summary of Findings

	IT Sabotage	Theft of Intellectual Property	Fraud
Target	Network, systems, or data	IP (trade secrets) – 71% Customer Info – 33%	PII or Customer Information
Access used	Unauthorized	Authorized	Authorized
When	Outside normal working hours	During normal working hours	During normal working hours
Where	Remote access	At work	At work
Recruited by outsiders	None	Less than 1/4	½ recruited for theft; less than 1/3 recruited for mod
Collusion	None	Almost ½ colluded with at least one insider; ½ acted alone	Mod: almost ½ colluded with another insider Theft: 2/3 colluded with outsiders

Common Sense Guide to Prevention and Detection of Insider Threats

http://www.cert.org/archive/pdf/CSG-V3.pdf

Summary of Best Practices in CSG

- Consider threats from insiders and business partners in enterprise-wide risk assessments.
- Clearly document and consistently enforce policies and controls.
- Institute periodic security awareness training for all employees.
- Monitor and respond to suspicious or disruptive behavior, beginning with the hiring process.
- Anticipate and manage negative workplace issues.
- Track and secure the physical environment.
- Implement strict password and account management policies and practices.
- Enforce separation of duties and least privilege.
- Consider insider threats in the software development life cycle.
- Use extra caution with system administrators and technical or privileged users.
- Implement system change controls.
- Log, monitor, and audit employee online actions.
- Use layered defense against remote attacks.
- Deactivate computer access following termination.
- Implement secure backup and recovery processes.
- Develop an insider incident response plan.

Polling Question

# 8 Does your organization have a dedicated group responsible for prevention, detection, and response to insider incidents? YES / NO

Publicly Available Information

Reports

Podcasts

Insider Threat Study

System Dynamics

E-Crime Watch Survey

(http://www.cert.org/insider_threat/)

Points of Contact

Insider Threat Technical Manager
Randall F. Trzeciak
CERT Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890
+1 412 268-7040 – Phone
rft@cert.org – Email

Greg Porter
Allegheny Digital
SEI Visiting Scientist
Telephone: +1 877-234-0001
Email: info@alleghenydigital.com

Insider Threat

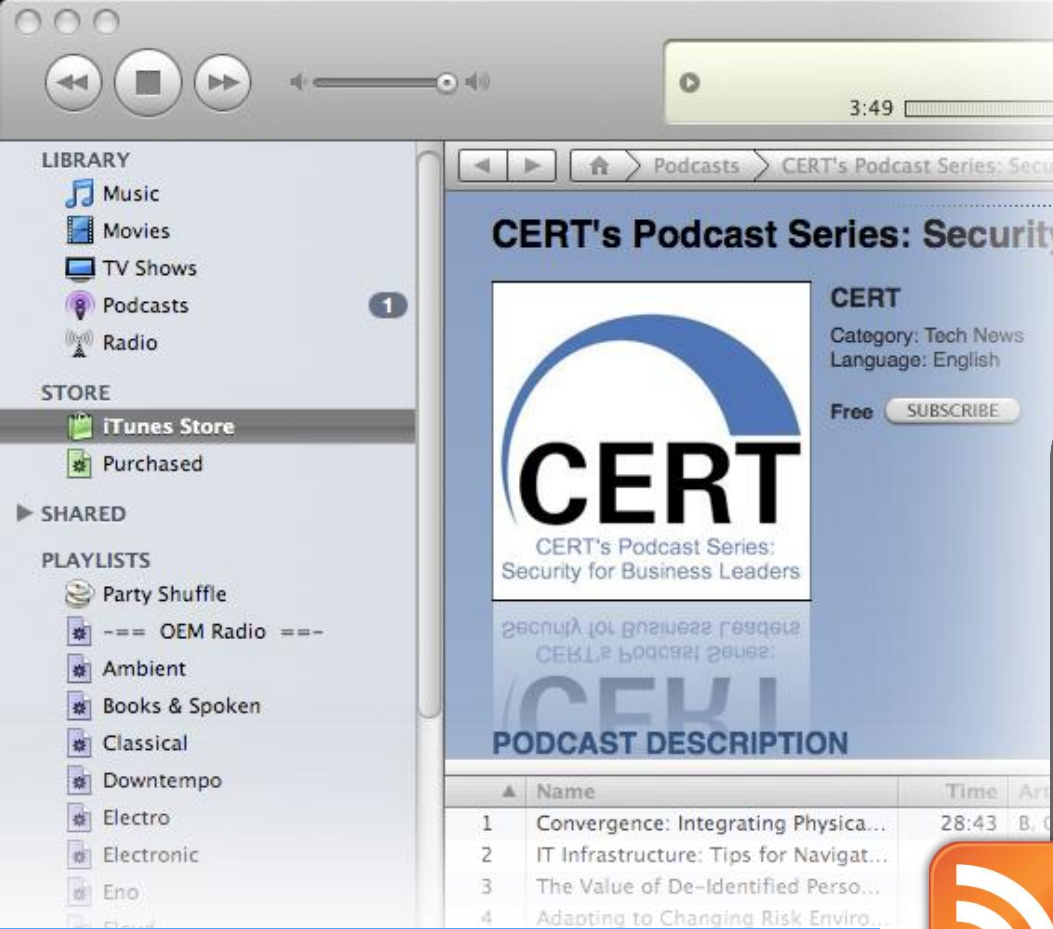
http://www.cert.org/insider_threat/

NO WARRANTY

GET THE BENEFITS OF CERT TRAINING

CERT works to create an international workforce skilled in information assurance and survivability by developing curricula on information assurance and security incident response for executives, managers, educators, software engineers, and network administrators and front-line system operators.

▶ www.cert.org/work/training.html



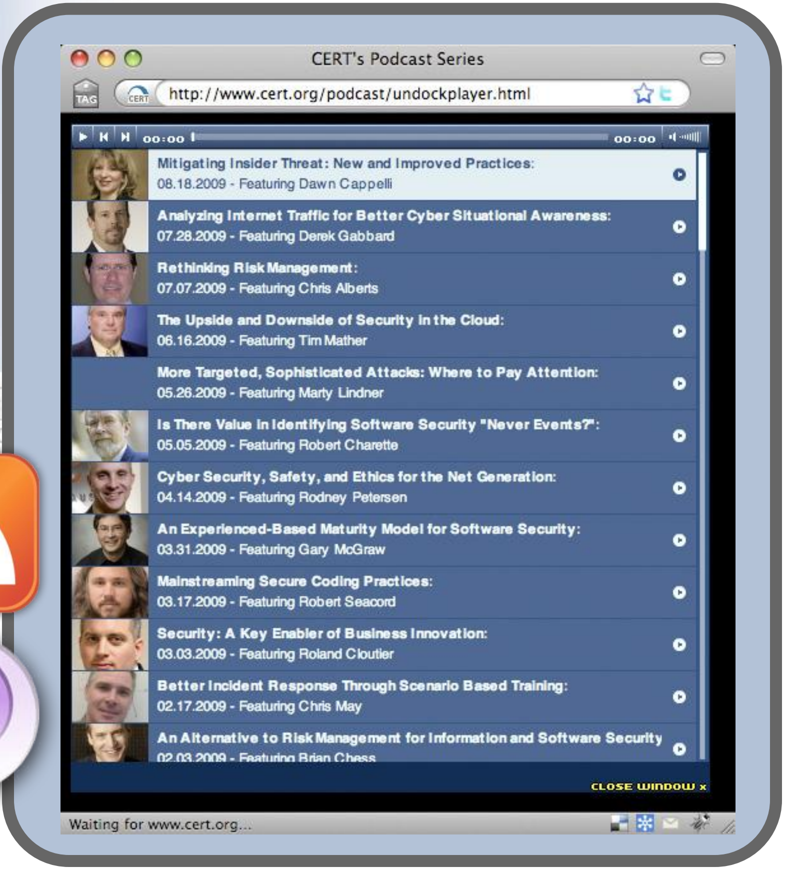
CERT's Podcast Series: Security for B

CERT

Category: Tech News
Language: English

PODCAST DESCRIPTION

	Name	Time	Art
1	Convergence: Integrating Physica…	28:43	B. C
2	IT Infrastructure: Tips for Navigat…		
3	The Value of De-Identified Perso…		
4	Adapting to Changing Risk Enviro…		



CERT's Podcast Series

http://www.cert.org/podcast/undockplayer.html

Mitigating Insider Threat: New and Improved Practices:
08.18.2009 - Featuring Dawn Cappelli

Analyzing Internet Traffic for Better Cyber Situational Awareness:
07.28.2009 - Featuring Derek Gabbard

Rethinking Risk Management:
07.07.2009 - Featuring Chris Alberts

The Upside and Downside of Security in the Cloud:
06.16.2009 - Featuring Tim Mather

More Targeted, Sophisticated Attacks: Where to Pay Attention:
05.26.2009 - Featuring Marty Lindner

Is There Value in Identifying Software Security "Never Events?":
05.05.2009 - Featuring Robert Charette

Cyber Security, Safety, and Ethics for the Net Generation:
04.14.2009 - Featuring Rodney Petersen

An Experienced-Based Maturity Model for Software Security:
03.31.2009 - Featuring Gary McGraw

Mainstreaming Secure Coding Practices:
03.17.2009 - Featuring Robert Seacord

Security: A Key Enabler of Business Innovation:
03.03.2009 - Featuring Roland Cloutier

Better Incident Response Through Scenario Based Training:
02.17.2009 - Featuring Chris May

An Alternative to Risk Management for Information and Software Security
02.03.2009 - Featuring Brian Chess

Waiting for www.cert.org...

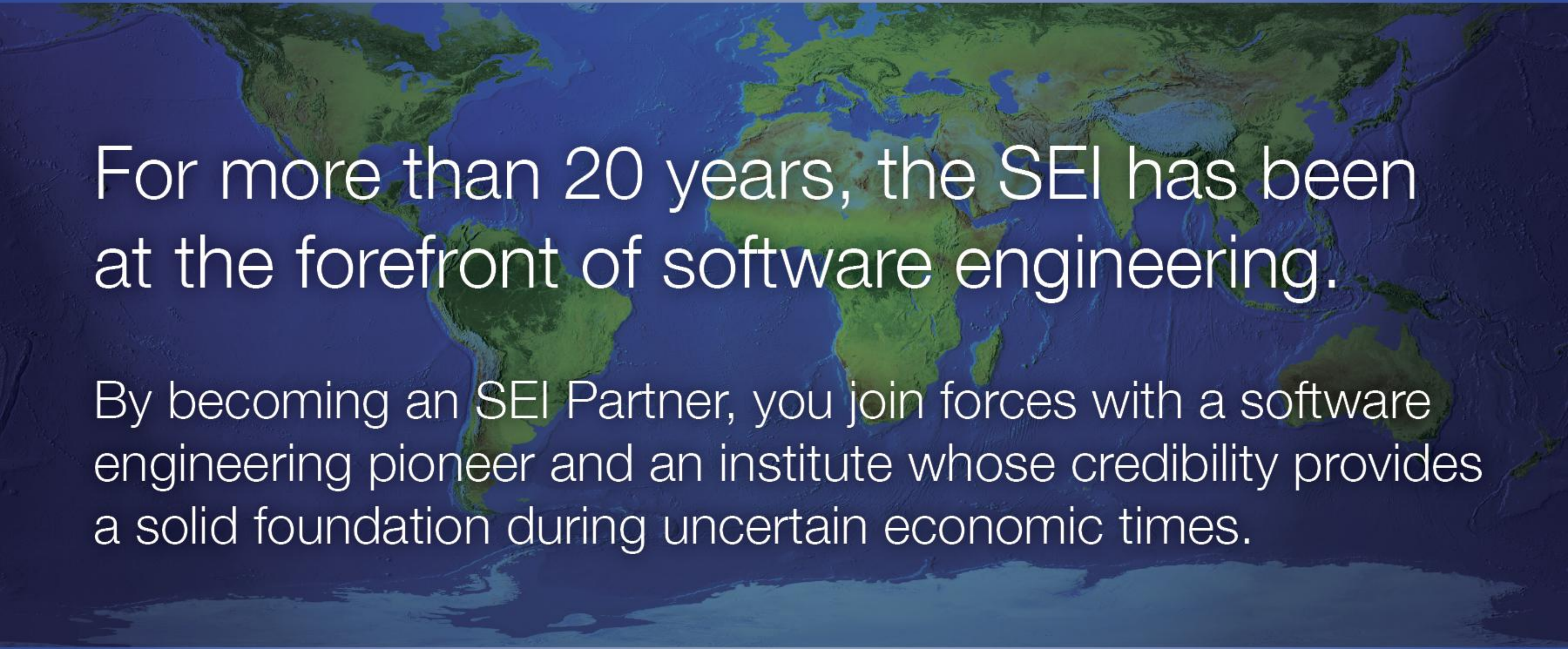
CERT's Podcast Series: Security for Business Leaders

www.cert.org/podcast/

Twitter: #seiwebinar

Become an SEI Member!

▶ www.sei.cmu.edu/membership



For more than 20 years, the SEI has been at the forefront of software engineering.

By becoming an SEI Partner, you join forces with a software engineering pioneer and an institute whose credibility provides a solid foundation during uncertain economic times.

SEI Partner Network

▶ www.sei.cmu.edu/partners